TECHNICAL JOURNAL Vol 1, No.1, July 2019
Nepal Engineers' Association, Gandaki Province
ISSN : 2676-1416 (Print)
Pp.: 10-15

ANALYSIS OF HYBRID CRYPTOSYSTEM DEVELOPED USING BLOWFISH AND ECC WITH DIFFERENT KEY SIZE

Suresh Timilsina, Sarmila Gautam*
Department of Electronics and Computer Engineering, TU, IOE, Paschimanchal Campus, Pokhara
** Department of Information and Technology, Pokhara Metropolitan City Office, Pokhara*

ABSTRACT

Hybridization is always done in search of better system which may not be always achieved. But most of the time hybridization has proved to produce a system with advantages of the algorithms used in developing that hybrid system. Even if the system doesn't have performance enhancement it will act as multi-layer security. Here, combing of Blowfish algorithm along with ECC algorithm is performed. After hybridization their performance analysis is done based on five different parameters with different key size of Blowfish algorithm i.e. 32 bit, 128 bit, 192 bit, 256 bit, 448 bit. Among these different hybrid cryptosystem we found that the Blowfish ECC system with key size 448 bit has better performance than all other bit size.

KEYWORDS: *Blowfish, ECC, Hybrid cryptography, Throughput*

INTRODUCTION

Cryptography is security science that deals with the art of hiding data. In communication, cryptography is one of the essential technique when communicating over any untrusted medium like internet where millions of attacker try to intrude highly secured information which is being shared between two or more other medium. There are two types of cryptosystem i.e. symmetric key cryptosystem and asymmetric key cryptosystem. Symmetric key cryptosystem is also known as private key cryptosystem whereas asymmetric key cryptosystem is also known as public key cryptosystem. But here we used the combination of symmetric key system and asymmetric key system to make a hybrid cryptographic system. The symmetric key cryptographic algorithm and asymmetric key cryptographic algorithm are used to form a strong dominating algorithm which comprises of both kinds into one system increasing the security level. But, security along with performance brings the best of each together and also minimize the disadvantages prevailing in each algorithm used individually. No matter it will certainly take some time but hybrid algorithm is not breached in finite life years. Here the concerned is just to find a best hybrid system among 5 system of same algorithms used but with different key size.

The main objectives of the system is as follows:

- To design hybrid cryptographic system using symmetric key algorithm and asymmetric key algorithm.
- To analyze the performance of the developed hybrid cryptosystem with different key length.

LITERATURE REVIEW

V. Kaur and A. Singh designed a hybrid system using AES as asymmetric key algorithm and ECC as symmetric key algorithm to obtain an improved AES and ECC which has high security with great performance but increased encryption and decryption time. [1] Khan and Khalid in 2013 researched and found that the average throughput of Blowfish was maximum as compared to individual AES and hybrid AES-Blowfish. The cipher encryption performance of AES and Blowfish was similar but the memory used by blowfish was found quite high. [2] This paper focus on the implementation of a system which is capable of encryption and decryption of multimedia data (Text, Images, Videos, Audio etc.) using a hybrid approach on the amalgamation of symmetric encryption techniques such as AES and asymmetric techniques such as ECC. ECC is based on the toughness of the discrete logarithm problem(DLP), whose public key is short, network bandwidth is little and has ability to resist to attacks is strong which makes it really difficult to guess the keys. Even if the attacker gets access to any of the keys, he or she won't be in a position to decrypt it in a relatively finite amount of life years. [3] Asymmetric algorithms like RSA, ECC and OAEP is compared in terms of their performance. Public key cryptography uses two keys one for encryption and other for decryption which provides better security. While comparing ECC and RSA it is found that ECC provides less overhead as compared to RSA. Similarly, in case of encrypting text ECC is better than RSA. In RSA, the message length must be less than the bit length. OAEP is padding scheme where there is no problem in message length and the encryption speed is better than RSA. [4] The ECC concept using with DH to solve the problem of key Exchange of the algorithm is called ECDHA. Limitation of this system is to decrease the throughput and thus data rate obtained is just compatibly with LTE. Algorithm using Hybrid Encryption and ECC" AES is found to be best symmetric encryption technology and more secure than the Blowfish algorithm. Blowfish gives high throughput as compared to AES and other algorithms. The hybrid of AES and Blowfish algorithm has characteristics of both the algorithms and it makes the algorithm strong against vulnerabilities. This hybrid structure of enhanced AES and Blowfish provides more security by increasing the complexity. ECC is the best algorithm of asymmetric encryption technology. The ECC is an emerging alternative for traditional Public-Key Cryptosystem like RSA. [5] Unlike all above references this paper focuses on comparative analysis of hybrid algorithm made from Blowfish and ECC algorithm. Here, the main factor affecting the performance is the key size of blowfish which ranges from 48 bit to 448 bit.

METHODOLOGY

A hybridization in cryptography is the combination of two cryptosystem using two different cryptographic algorithm namely symmetric key cryptographic algorithm and asymmetric key cryptographic algorithm to form a strong dominating algorithm which comprises of both kinds into one system increasing the strength. A hybrid algorithm can even be made combining all symmetric algorithms, all asymmetric algorithms or mixer of both type of algorithms. Hybrid algorithm is considered highly secure as long as the public and private keys are secure. Hybridization will always not make higher performance result but for sure the security of the system will be highly increased.

Blowfish-ECC hybridization:

Blowfish-ECC hybridization is made from combination of a symmetric key algorithm i.e.

Blowfish and an asymmetric key algorithm i.e. ECC.

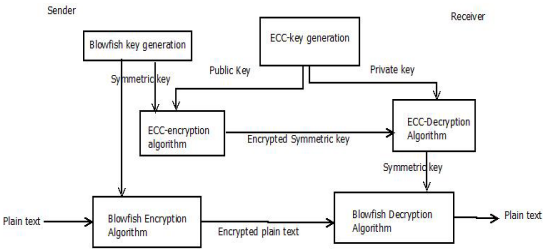

Figure 1: Block diagram of hybrid system using Blowfish and ECC algorithm

Here, first the key is generated of one size among 32 bit – 448 bit for blowfish algorithm which is then used to encrypt the plain text provided. The key is now encrypted using public key i.e. ECC. Both the encrypted key as well as encrypted plain text is transmitted to receiver section where the encrypted key is decrypted using private key. Thus, the then decrypted key is used to decrypt the plain text. After the system is made. This system is used to analyze various parameters for different key size.

Throughput: The calculation of throughput is done using encryption time of the plain text. It resemble the speed of encryption. The throughput is the ratio of total plain text to total encryption time. Throughput can also be calculated in terms of decryption time and cipher text.

$$\text{Throughput} = \frac{Tp}{Et}$$

Where T_p= Size of plain text + size of symmetric key

Et= Plain text encryption time + symmetric key encryption time

Plaintext size to cipher text size: It is the ratio of plaintext size to that of cipher text size. In case of hybrid algorithm plaintext size is the sum of size of plaintext and symmetric key. Similarly, the cipher text size is the sum of size of encrypted plaintext and encrypted symmetric key.

Total Execution Time: It is the total time required for Encryption of a plain text (i.e. combination of plaintext and symmetric key) and decryption of cipher text (i.e. combination of encrypted plaintext and encrypted symmetric key) using a hybrid cryptographic.

Encryption Time: It is the time required for encryption of plain text (i.e. combination of plaintext and symmetric key) using hybrid

algorithm.

Decryption Time: It is the time required for decryption of cipher text (i.e. combination of encrypted plaintext and encrypted symmetric key) using hybrid algorithm.

RESULT AND DISSCUSSION

Here, symmetric and asymmetric key algorithm are used for hybrid cryptographic algorithm are made. After that the performance analysis of the system are carried out on the basis of following parameters. Throughput is the ratio of total plain text to total encryption time. It can also be calculated in terms of decryption time and cipher text. In case of hybrid algorithm plaintext size is the sum of size of plaintext and symmetric key. Total Execution Time is the total time required for Encryption of a plain text (i.e. combination of plaintext and symmetric key) and decryption of cipher text (i.e. combination of encrypted plaintext and encrypted symmetric key) using a hybrid cryptographic. Encryption Time is the time required for encryption of plain text (i.e. combination of plaintext and symmetric key) using hybrid algorithm. Decryption time is the time required for decryption of cipher text (i.e. combination of encrypted plaintext and encrypted symmetric key) using hybrid algorithm.

Table 1: Various data of hybrid Blowfish-ECC system with different key length

Algorithm	Total P-text (bits)	Total C-text (bits)	Plain-text to cipher ratio	Total E-time (Sec)	Total D-Time (Sec)	Total Exe Time (Sec)	Throughput
B-ECC(32)	352	539	0.65306	0.04799	0.042747	0.090741	7334.357
B-ECC (128)	448	539	0.83116	0.05538	0.050930	0.106313	8089.1963
B-ECC (192)	512	539	0.94990	0.04426	0.039287	0.083554	11566.151
B-ECC (256)	576	692	0.83236	0.05086	0.041376	0.092243	11323.781
B-ECC (448)	768	849	0.904593	0.05050	0.039415	0.089918	15207.137

From above table 1 we can see that for a same message the total plain text size increased on increasing the size of key. Similarly the cipher text size is slightly more than the plain text size but with same increasing nature with increase in key size for 256 and 448 bit key but it remained same for key size 32-192 bit key size. The execution time for Blowfish –ECC with key size 192 bit is found to be least as compared to other hybrid algorithms with different key size this is because there is not much difference in size of total plain text and total cipher text. The decryption time for Blowfish-ECC with key size 448 bit is found to be least. Similarly the throughput is maximum for the hybrid algorithm with key size 448 bit.

Table 2: Entropy of Hybrid Blowfish- ECC with different key size

Hybrid algorithm	Sk-size	Entropy of E-msg	Entropy (E-Skey)
Blowfish-ECC	32	3.9614	3.2814
Blowfish-ECC	128	3.9355	3.2836
Blowfish-ECC	192	3.8872	3.2964
Blowfish-ECC	256	3.8935	3.2753
Blowfish-ECC	448	3.8635	3.3024

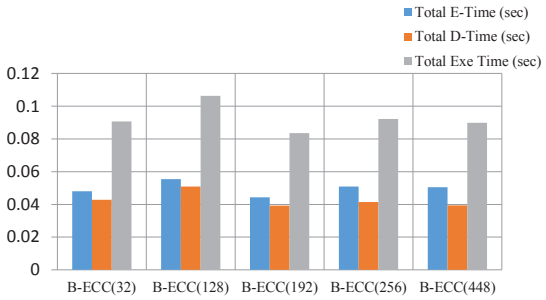

Figure 2: Bar Chart for hybrid algorithm to show total encryption time, total decryption time and total execution time

The graph shows that the total encryption time , total decryption time and the total execution time of the blowfish ECC algorithm is best being least for the key size of 192 bit. And that of key size 128 bit is with greater encryption time, decryption time and execution time during the hybridization with Blowfish and RSA algorithm.

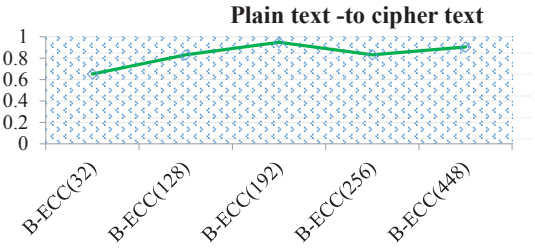

Figure 3: Line graph for hybrid algorithm to show plain text to cipher text size

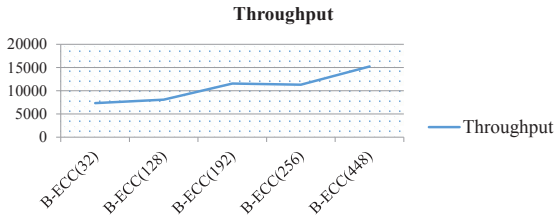

Figure 4: Line graph for hybrid algorithm to show Throughput

The plain text to cipher text ratio is also found to be greater with key size of 192 bit but the throughput shows increased with the increment in the the size of key from 32 to 448 from 7334.357 to 15207.137.

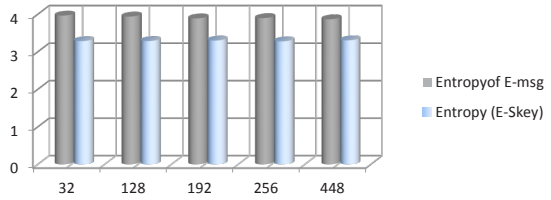

Figure 5: Bar graph for hybrid algorithm to show Entropy

Figure 5 shows that the entropy of message is higher than the symmetry key with every key size. But there is very little variation on entropy among entropy of messages at different key and among entropy of symmetry key at different key size while using Blowfish ECC algorithm.

CONCLUSION

From all above data it is clearly seen that the hybrid algorithm is safe no doubt then a single algorithm but among the hybrid system made using Blowfish and ECC algorithm with different key size Blowfish- ECC with key size 448 bit has better performance in terms of throughput whereas the Blowfish-ECC with key size 192 is found to have better performance in terms of Execution time, decryption time and Encryption time.

REFERENCES

[1] V. Kaur and A. Singh, "*Review of Various Algorithms Used in Hybrid Cryptography*", International Journal of Computer Science and Network December 2013, vol. 2, no. 6, pp. 157–173, 2013.

[2] M. Ebrahim, S. Khan, and U. B. Khalid, "Symmetric Algorithm Survey: A Comparative Analysis," International Journal of Computer Applications, vol. 61, pp. 12–18, 2013.

[3] S.C.Iyer, R.R.Sedamkar and S.Gupta, "Multimedia Encryption using Hybrid Cryptographic Approach," International Journal of Computer Applications, May 2013, vol 56.

[4] N. Garg and P. Yadav, "*Comparison of Asymmetric Algorithms in Cryptography*," International Journal of Computer Science and Mobile Computing, vol. 3, no. 4, pp. 1190–1196, 2014.

[5] A.P Shaikh, V. kaul, "*Enhanced Security Algorithm using Hybrid Encryption and ECC*," IOSR Journal of Computer Engineering, vol. 16, Issue 3, pp. 80-85,May-Jun. 2014.